SCHEDULE 1

1. Definitions & Interpretation

1.1 Definitions:

Confidential Information: any and all information whether about the Consultant, ROS, ROS Client or any other party which is confidential in nature without regard to the manner in which it reached the Consultant or ROS, as the case may be, including:

a. any Engagement and Services under this Agreement save for the terms of this umbrella agreement as such.
b. property, business, customers and suppliers, trading practices, trade secrets, know-how, plans, proposals and prospects, processes and safety and security incidents, measures and/or exposures of a Party;
c. information about the functionality, capacity and response times of ROS Client Systems and or ROS Systems, including service trouble, interruption and downtime, viruses, disabling codes, attacks, ransomware, phishing events, security breaches, backdoors, threats, programming errors, service denial events, contingency plans, backups;
d. information about suppliers, licenses and claims as well as proprietary information about ROS Clients applications and services and those of ROS.
e. all access information to ROS Clients Systems or ROS' Systems, whether obtained to perform the Services or in the process of performing the Services specially including information in connection with phishing training, including test accounts, test environment and contact information of system administrators, in case of emergencies;
f. the information specified as confidential in clause 7; and
g. data, software, source code, documentation, other spoken and written information which may become known to a Party under this Agreement.

Confidential Information does not include information that is public at the time of disclosure or becomes generally known without this Agreement having been violated.

Computing Infrastructure means the foundation or framework supporting a system or organisation for the flow, storage, processing and analysis of data whether composed of physical or virtual resources, centralised or decentralised, with one or more data centres that are controlled by the organisation or for them by a third party, such as a colocation facility or cloud provider.

Engagement: are agreements to perform certain Services for ROS Clients agreed from time to time between the Parties, to be performed in accordance with the terms of this Agreement and the Specifications.

Intellectual Property Rights: for the purposes of the Agreement means all copyright and other intellectual property rights in whatever material or media whether or not registered including, without limitation, system software, application software, interfaces, models, detailed technical documentation and specifications, data models, algorithms, object code, source-code, data base, data and compilation rights, rights in know-how and trade secrets and any other computing solutions.

Rate: the rate ROS and the Consultant agree in written form for an Engagement.

ROS Client: any person or entity with which ROS has concluded a written contract to provide cyber security services.

ROS Policies: include policies about information security, access control, patch management policies, healthy working environment as well as the GDPR protocols, ROS Core Principles and ROS General Terms and Conditions. They are made available to the Consultant by publication. The ROS Policies that are current at the time of signing this Agreement are in Schedule 3.

ROS General Terms and Conditions are the general terms and conditions of ROS which at the time of this Agreement is version 1.0 Date 14-07-2014 as amended from time to time in accordance with the then current ROS change management process and procedures.

Services: are services under this Agreement as further specified in the Schedule 2. The services are intended to gain insight into the security of ROS Clients' systems. To do so, access will be had to these systems, to attempt to find vulnerabilities, and gain further access and elevated privileges by exploiting any vulnerabilities found.

Specifications: are the written parameters of the Services to be provided in an Engagement including about the ROS client, the system, type of testing, time and duration of testing, milestones and planning, agreed number of hours to be spent, reporting methodology and costs, as determined by the relevant scoping services (in Schedule 2).

Taxes: means any and all applicable tax or taxes (including, but not limited to, any value added tax, sales tax, income tax, or business tax, stamp or other duty, levy, impost, charge, fee, deduction, penalty or withholding imposed levied, collected or assessed) and includes interest thereon.

1.2 Interpretation:

a. References to clauses and Schedules shall be references to clauses and schedules to this Agreement, unless the context expressly, or by necessary implication, otherwise requires.
b. All Schedules to this Agreement shall form an integral part hereof.
c. English language words used in this Agreement intend to describe Dutch legal concepts only and the consequences of the use of those words in English law or any other law shall be disregarded.
d. A reference to any statute, or any particular provision or provisions of a statute, includes any amendment, replacement or re-enactment thereof for the time being in force and any by-laws, statutory instruments, rules, regulations, notices, orders, directions, consents or permissions made there under and any conditions attaching thereto.
e. Any reference to a Schedule includes any amendment and/or replacement thereof.
f. The singular includes the plural and vice versa.
g. A reference to any currency or € is to euro.
h. A reference to a person includes a reference to the person's executors, administrators, substitutes, successors and permitted assigns.
i. A reference to a person includes a reference to a natural person, body corporate, joint venture, partnership or statutory entity.
j. Headings in this Agreement are for convenience only and do not affect the construction or interpretation of this Agreement.

SCHEDULE 2

Non-exhaustive list of Services

Below is a list of services that are Services under this Agreement. To understand what the Services entail, reference is made to industry standards that may from time to time change. The standard to be adhered to is the standard at the time of providing the Services.

a) **Scoping;**
A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security controls in the security control baseline. Areas of consideration include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective. Source: https://csrc.nist.gov/glossary/term/scoping_considerations

b) Penetration testing;
Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. Source: https://csrc.nist.gov/glossary/term/penetration_testing

Penetration testing standard: http://www.pentest-standard.org/index.php/Main_Page

c) Red team assignments;

Red team: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team. Source: https://csrc.nist.gov/glossary/term/red_team

d) Social engineering/phishing engagements; and **Social engineering:** An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. Source: https://csrc.nist.gov/glossary/term/social_engineering

e) Phishing: A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. Source: https://csrc.nist.gov/glossary/term/phishing

f) Incident response;
The mitigation of violations of security policies and recommended practices. Source: https://csrc.nist.gov/glossary/term/incident_response

g) Forensics;
The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. Source: https://csrc.nist.gov/glossary/term/forensics

h) Custom R&D;
Research and design. Source: https://csrc.nist.gov/glossary/term/randd

i) Compliance support;
A comprehensive review of an organization's adherence to governing documents such as whether a Certification Practice Statement satisfies the requirements of a Certificate Policy and whether an organization adheres to its Certification Practice Statement. Source: https://csrc.nist.gov/glossary/term/compliance_audit

j) Audit preparation;
Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. Source: https://csrc.nist.gov/glossary/term/audit

k) Code audit (analysis);
The act of reverse-engineering the malicious program to understand the code that implements the software behavior. For example, when looking at compiled programs, the process involves using a disassembler, a debugger, and perhaps a decompiler to examine the program's low-level assembly or byte-code instructions. A disassembler converts the instructions from their binary form into the human-readable assembly form. A decompiler attempts to recreate the original source code of the program. A debugger allows the analyst to step through the code, interacting with it, and observing the effects of its instructions to understand its purpose. Source: https://csrc.nist.gov/glossary/term/code_analysis\

l) Training/workshops;
The 'Training' level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing). Source: https://csrc.nist.gov/glossary/term/training

m) Generic consulting;
The activity of giving advice on a particular subject. Source: https://dictionary.cambridge.org/dictionary/english/consultancy

n) Infra (system administration for ROS itself);
An individual, group, or organization responsible for setting up and maintaining a system or specific system elements, implements approved secure baseline configurations, incorporates secure configuration settings for IT products, and conducts/assists with configuration monitoring activities as needed. Sound implementation of established Information security policies and procedures. Source: https://csrc.nist.gov/glossary/term/system_administrator

o) Project Management services:
The activity of organizing and controlling a project. Source: https://dictionary.cambridge.org/dictionary/english/project-management

SCHEDULE 3

ROS Policies

Notes to reader:
1. ROS Policies may be amended from time to time, new policies may be adopted and policies may be terminated.
2. Each ROS Policy has a time and date stamp.
3. ROS will adhere to its change management processes for amending, adopting and terminating ROS Policies.
4. The current version and previous version of ROS Policies can be found at on GitHub and our GitLab internal onboarding repository.

GDPR protocols	**Information security policies**
1. (Personal) data breach protocol	1. Access control policy
2. Disaster recovery protocol	2. CVD policy
3. Encryption protocol	3. Information security policy
4. Phishing protocol	4. Password policy
5. Data retention policy	5. Patch management policy
6. Testing and evaluation protocol	
7. Technical and organizational measures	

ROS Policies and protocols (sanitized versions):
https://github.com/radicallyopensecurity/publications/tree/main/policies-and-protocols

ROS Core Principles
ROS has a number of values that are described as ROS "**Core Principles**." These are:

No sketchy stuff
ROS doesn't build surveillance systems, hack activists, sell exploits to intelligence agencies, or anything like that. If a job is even remotely morally questionable, we simply won't do it.

Open-Source
Releasing ALL tools and frameworks ROS builds as open source.

Teach to fish
During engagements, ROS will not only share the results with the ROS Client, but provide a step-by-step description of how to perform the same audit or procedure without ROS. ROS wants to demystify what we're doing. It's not rocket science, and ROS genuinely wants to help customers improve their security posture, even if it costs ROS repeat business.

IoCs for free
Releasing ALL collected threat intelligence (Indicators of Compromise) into an open-source database that everyone can freely use. (Sanitized in agreement with customers.)

Zero days
ROS doesn't sell zero-days - we responsibly disclose them!

For clarity in the context of this Agreement, the ‘open source’ Core Principle above, refers to ROS ‘s intention to use GPL where suitable in its reasonable opinion. Other open source methodologies are constantly monitored for possible benefits and use in any given circumstances.